BITA RAHEBI (CA SBN 209351)
brahebi@mofo.com
RYAN J. MALLOY (CA SBN 253512)
rmalloy@mofo.com
ROSE S. LEE (CA SBN 294658)
roselee@mofo.com
NIMA KIAEI (CA SBN 336142)
nkiaei@mofo.com
MORRISON & FOERSTER LLP
707 Wilshire Boulevard
Los Angeles, California 90017-3543
Telephone: (213) 892-5200
Facsimile: (213) 892-5454

RICHARD S.J. HUNG (CA SBN 197425)
rhung@mofo.com
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105
Telephone: (415) 268-7000
Facsimile: (415) 268-7522

Attorneys for Defendant
APPLE INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MPH Technologies Oy,

Plaintiff,

v.

Apple Inc.,

Defendant.

Case No. 3:18-cv-05935-TLT

**APPLE'S RESPONSIVE CLAIM CONSTRUCTION BRIEF**

Date: December 11, 2023
Time: 11:00 a.m.
Courtroom: 9
Judge: Hon. Trina L. Thompson

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

**Page(s)**

**Cases**

**Rules**

## I. INTRODUCTION

MPH seeks to expand its patents to cover systems and methods that the applicants did not invent. For example, MPH contends that the terms "exchange" and "negotiating" require no interaction at all and that the IPSec security protocol that the applicants called "essential" is actually optional.

Apple's constructions, by contrast, are properly rooted in the claim language, the specifications, and the prosecution histories. Apple's constructions generally result in claims consistent with what the applicants said they invented, with the exception of claims that have structural errors rendering them indefinite. The Court should adopt Apple's constructions.

## II. MPH'S ASSERTED PATENTS

MPH's patents, which originate from applications filed in 2001 and 2002, are all directed to one problem: how to modify the existing IPSec protocol to handle mobile devices. (*See* '949 patent, 4:27-28[1] ("The problem with standard IPSec is thus that it has been designed for static connections."); '581 patent, 4:36-37 ("The problem with standard IPSec tunnel end points are that they are fixed."); '302 patent, 4:55-56 ("IPSec does not work well with mobile devices.").) As discussed below, each patent discloses a modification to IPSec to accommodate mobile devices.

### A. The Claimed Invention of the Intermediate Computer Patents

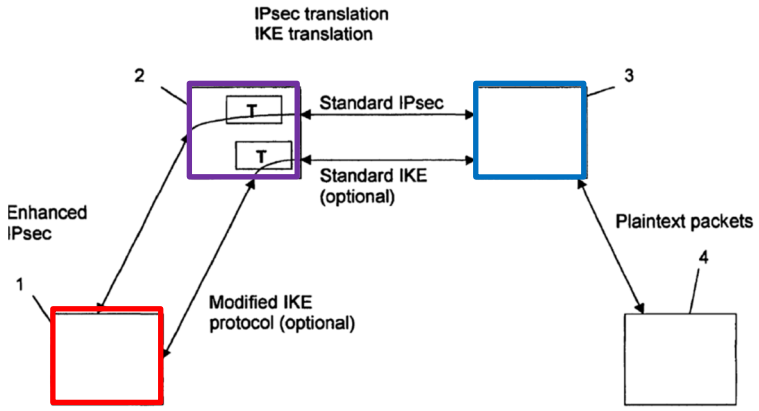


**FIG. 1**

(Box 1 = first computer; Box 2 = intermediate computer; Box 3 = second computer)

[1] The '949, '397, '494, '502, and '362 patents ("Intermediate Computer Patents") share the same specification. For convenience and simplicity, Apple cites only to the '949 specification.

The Intermediate Computer Patents disclose positioning an "intermediate computer" between the sending and receiving devices (a.k.a. "first computer" and "second computer"). (*E.g.*, '949 patent, 6:27-30; Fig. 1 (annotated above).) The specification explains that "***[a]n essential idea*** of the invention is to use the standard protocol (***IPSec***) between the intermediate computer and the second computer and an 'enhanced ***IPSec*** protocol' between the first computer and the intermediate computer." (*Id.*, 7:29-32.[2]) The "enhanced" IPSec protocol, unlike the standard one, enables updates when the first computer changes addresses. (*Id.*, 7:37-60.)

The intermediate computer uses a translation table to convert the variable parameters of its "enhanced" IPSec connection with the first computer into the static parameters of its "standard" IPSec connection with the second computer. (*Id.*, 7:32-46.) The converted parameters include IP addresses and IPSec-specific parameters called "SPI values." (*Id.*, 7:37-41.) The specification provides a detailed explanation of how the intermediate computer translates IP addresses and SPI values. (*Id.*, 11:23-12:11.) The specification does not discuss any non-IPSec embodiment.

**B. The Claimed Invention of the '581 Patent**

The specification of the '581 patent declares that "[t]he applicant has solved the above problems of prior art by defining a signalling [sic] mechanism that allows ***an existing IPSec security association***, that is, the symmetric encryption and authentication algorithms used for packet processing, along with their keys and other parameters, to be moved from one network to another." ('581 patent, 7:23-28.) The specification provides details about this signaling mechanism that go beyond the present claim construction disputes. (*Id.*, 7:38-8:12.)

**C. The Claimed Invention of the '302 Patent**

The '302 patent's solution to the IPSec mobility problem is for a mobile device to form multiple IPSec connections. (*See* '302 patent, 7:21-33.) When the mobile device changes addresses, it can use a preexisting connection instead of establishing a new connection, which the specification says is time consuming and computationally expensive. (*Id.* at 3:24-30, 7:21-33.)

[2] All emphasis herein is added unless stated otherwise.

## III. PRINCIPLES OF CLAIM CONSTRUCTION

"When construing claim terms, we first look to, and primarily rely on, the intrinsic evidence, including the claims themselves, the specification, and the prosecution history of the patent, which is usually dispositive." *Sunovion Pharms., Inc. v. Teva Pharms. USA, Inc.*, 731 F.3d 1271, 1276 (Fed. Cir. 2013). "The specification is *always* highly relevant to the claim construction analysis and is, in fact, the single best guide to the meaning of a disputed term." *Trs. of Columbia Univ. v. Symantec Corp.*, 811 F.3d 1359, 1363 (Fed. Cir. 2016) (italics in original, internal quotation marks omitted); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc). A court may consider extrinsic evidence "as long as those sources are not used to contradict claim meaning that is unambiguous in light of the intrinsic evidence." *Phillips*, 415 F.3d at 1324.

## IV. PROPER CONSTRUCTION OF DISPUTED CLAIM TERMS

### A. "Secure" terms (all patents)

| Claim Term | MPH's Construction | Apple's Construction |
|---|---|---|
| **"secure connection"** | "connection protected by [the] one or more security protocols" | "IPSec connection" / otherwise indefinite |
| **"secure[ly] forward[ing]"** | plain and ordinary meaning, needs no construction[3] | "Forward[ing] using IPSec connection" / otherwise indefinite |
| **"secure message"** | plain and ordinary meaning, needs no construction. Alternatively: "message protected by [the] one or more security protocols" | "IPSec message" - / otherwise indefinite |

The "secure" terms appear throughout MPH's patents. Apple focuses its analysis below on the Intermediate Computer Patents and concludes the analysis with a discussion specific to the '581 and '302 patents, which raise similar issues.

[3] For space and clarity, Apple has deleted MPH's positions that this term is not a limitation when it appears solely in the preambles of certain claim terms. Apple does not dispute that.

**1. The "secure" terms in the Intermediate Computer Patents should be construed to require IPsec because the patents characterize the purported invention as a system that uses IPsec and do not disclose any non-IPsec embodiments.**

The primary question the Court must decide for the "secure" terms is whether they should be construed to require what the specification for the Intermediate Computer Patents explicitly says is "essential" to the invention—IPsec. Federal Circuit law is clear: Yes, they should.

The Federal Circuit has consistently held that a specification's descriptions of the invention as a whole act to limit the scope of the claims. For example, in *GPNE Corp. v. Apple Inc.*, 830 F.3d 1365 (Fed. Cir. 2016), the court instructed: "When a patent . . . describes the features of the 'present invention' as a whole, this description limits the scope of the invention[.]" *Id.* at 1371 (quoting *Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1308 (Fed. Cir. 2007)). There, GPNE argued that a narrow construction of "node" requiring the capability to "operate[] independently from a telephone network" was improper because it was based on a "single summation sentence" from the specification. *Id.* at 1371. The Federal Circuit disagreed, because that sentence described "the invention" as a whole as having that capability. *Id.*

Similarly, in *Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340 (Fed. Cir. 2004), the Federal Circuit construed "sending," "transmitting," and "receiving" to require communication over a telephone line due to "clear statements in the specification that the invention . . . is directed to communications 'over a standard telephone line.'" *Id.* at 1348-49. The court explained: "We cannot construe the claims to cover subject matter broader than that which the patentee itself regarded as comprising its inventions and represented to the PTO." *Id.* at 1349.

The *GPNE* and *Microsoft* cases are but two examples of the Federal Circuit's many consistent holdings. *See, e.g.*, *Lemoine v. Mossberg Corp.*, No. 2020-2140, 2021 WL 4199934, at *3 (Fed. Cir. Sept. 15, 2021) (construing "converting" to require retrofitting where specification stated that the invention related to retrofitting); *Verizon*, 503 F.3d at 1308 (construing "localized wireless gateway system" to require that the gateway perform compression and packetization where specification stated that the invention required those activities); *Andersen Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1365-68 (Fed. Cir. 2007) (construing "composite composition"

to require a pellet or linear extrudate form because specification made clear invention required that); *Honeywell*, 452 F.3d at 1318 (limiting "fuel injection system component" to a fuel filter where specification "refer[red] to the fuel filter as 'this invention' or 'the present invention'"); *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 864 (Fed. Cir. 2004) (construing "plug" to require pleats where Summary of the Invention stated that the invention "includes a pleated surface"); *SciMed Life Sys., Inc. v. Advanced Cardiovascular Sys., Inc.*, 242 F.3d 1337, 1343 (Fed. Cir. 2001) (restricting claims to specific "coaxial" configuration due to specification's discussion of "the present invention"). These holdings flow naturally from the more general rule that "[c]laims must be read in view of the specification, of which they are a part." *See, e.g.*, *Honeywell*, 452 F.3d at 1318 (quoting *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc) (alterations omitted)).

Here, the specification is unequivocal that the invention requires IPSec. The Summary of the Invention states: "***An essential idea of the invention is to use the standard protocol (IPSec)*** between the intermediate computer and the second computer and an 'enhanced ***IPSec*** protocol' between the first computer and the intermediate computer. ***IPsec***-protected packets are translated by the intermediate computer, without undoing the ***IPsec*** processing." ('949 patent, 7:29-34.) *See C.R. Bard*, 388 F.3d at 864 ("Statements that describe the invention as a whole are more likely to be found in certain sections of the specification, such as the Summary of the Invention."). The Summary of the Invention continues that "***the system of the invention***" "is characterized in that the first and the second computers have means to perform ***IPSec*** processing, and the intermediate computer have means to perform ***IPSec*** translation . . . ." ('949 patent, 8:32-39.)

The remainder of the specification is also unequivocal. The specification states that "***in the invention***, an ***IPSec*** connection is shared by the first computer and the second computer, while the intermediate computer holds information required to perform address and ***IPSec*** SPI translations for the packets." ('949 patent, 10:11-15.) It further states that the key exchange in the invention "***must*** establish not only cryptographic keys, but also the ***IPSec*** translation table entries." (*Id.*, 14:21-24.) It declares that "[t]he advantage of ***the invention*** is that the logical

***IPSec*** connection ***shared*** by the first and the second computer can be enhanced by the first and the intermediate computer without involvement of the second computer." (*Id.*, 10:24-27.)

These statements limiting the invention to IPSec are at least as clear and unequivocal as those in the Federal Circuit cases discussed above. The patentee said that IPSec is "essential," and "[t]he public is entitled to take the patentee at his word." *Honeywell*, 452 F.3d at 1318.

MPH misconstrues the specification's statement that "[t]he invention is not restricted to . . . any existing protocols, such as the currently standardized IPSec or IKE." (Br. at 8-9 (citing '949 patent, 9:26-33).) This simply means that the invention could be used with later versions of IPSec (which uses IKE for key exchange) than existed at the time of filing.

MPH also cites a sentence that reads: "Preferably, the secure message is formed by making use of the IPSec protocols . . . ." (Br. at 9 (citing '949 patent, 6:45-67).) But shortly thereafter, the specification clarifies that IPSec is "essential" to the invention. ('949 patent, 7:29-32.) The explicit statement that IPSec is "essential" outweighs any inference that IPSec is optional, especially given that the specification identifies no alternative. *See In re Acacia Media Techs. Corp.*, No. C 05-01114, 2008 WL 413747, at *5 (N.D. Cal. Feb. 13, 2008) (finding that "preferably" phrase did not negate statements that feature was essential to invention).

**2. Construing the "secure" terms to require IPSec provides an antecedent basis for claim 8 of the '949 patent.**

Further support for construing the "secure" terms to require IPSec is that doing so provides the necessary antecedent basis for claim 8 of the '949 patent. "The requirement of antecedent basis is a rule of patent drafting, administered during patent examination." *Energizer Holdings, Inc. v. Int'l Trade Comm'n*, 435 F.3d 1366, 1370 (Fed. Cir. 2006). "In order to provide an explicit antecedent basis, a claim must introduce a given term using an indefinite article (e.g., 'a' or 'an') before referring to it in definite form, using 'the' or 'said.'" *Comcast Cable Commc'ns, LLC v. Sprint Commc'ns Co., LP*, 38 F. Supp. 3d 589, 616 (E.D. Pa. 2014). The lack of an antecedent basis is grounds for finding a claim invalid for indefiniteness. *See, e.g.*, *Bushnell Hawthorne, LLC v. Cisco Sys., Inc.*, 813 F. App'x 522, 526-27 (Fed. Cir. 2020).

Claim 8 of the '949 patent states: "The method of claim 1 wherein the method further comprises ***the* IPSec connection** being one or more security associations (SA) and the unique identity being one or more SPI values." "The IPSec connection" needs an antecedent basis, but neither claim 1 nor claim 8 explicitly recites an "IPSec connection." This evidences the patentee's intent to use "secure connection" in claim 1 to provide that antecedent basis. Construing "secure connection" to mean an IPSec connection accords with the patentee's intent and saves claim 8 from indefiniteness. *See JBF Interlude 2009 Ltd. v. Quibi Holdings LLC*, No. 22:20-CV-2250, 2021 WL 1390367, at *14 (C.D. Cal. Apr. 12, 2021) (construing term in independent claim to provide antecedent basis for term in dependent claim).

**3. MPH's claim language arguments are unavailing.**

MPH incorrectly argues that because some claims recite IPsec, other claims cannot require it. (Br. at 7-8.) "Claim differentiation is 'not a hard and fast rule,' but rather a presumption that will be overcome when the specification or prosecution history dictates a contrary construction." *GPNE*, 830 F.3d at 1371 (construing "node" to mean pager even though other claims recited "pager") (quoting *Seachange Int'l, Inc. v. C-COR, Inc.*, 413 F.3d 1361, 1369 (Fed. Cir. 2005)).

The Federal Circuit's *Andersen* decision is instructive. Some independent claims there recited a "pellet" or "extrudate," while others did not. 474 F.3d at 1369-70. (*See also* Ex. A (*Andersen* patent – U.S. Patent No. 5,932,334) at claims 1, 10, and 19.)[4] The patentee argued that the other claims could not be limited to a pellet or extrudate. The Federal Circuit disagreed and explained: "we have held that 'the written description and prosecution history overcome any presumption arising from the doctrine of claim differentiation.'" *Id.* at 1370 (quoting *Kraft Foods, Inc. v. Int'l Trading Co.*, 203 F.3d 1362, 1368 (Fed. Cir. 2000)). The court noted that "overlapping patent claims are not unusual." *Id.*

The Federal Circuit's decision in *Edwards Lifesciences LLC v. Cook Inc.*, 582 F.3d 1322 (Fed. Cir. 2009) is also instructive. There, the patentee argued that because a dependent claim recited a "wire structure," the independent claim could not require a wire structure. *Id.* at

[4] All citations of the form "Ex. [#]" are to the Declaration of Ryan Malloy.

1331-32. The Federal Circuit rejected that argument because the specification made clear that the claimed invention required wires. *Id.*; *see also Howmedica Osteonics Corp. v. Zimmer, Inc.*, 822 F.3d 1312, 1323 (Fed. Cir. 2016) ("Although it is a useful tool, claim differentiation does not require that the 'dependent claim tail . . . wag the independent claim dog' in this case.").

MPH incorrectly argues that its claims cannot require IPSec because '949 claim 3 and '494 claims 6 and 7 recite the use of different protocols (SSL and TLS). (Br. at 7.) MPH's argument is based on an unfounded assumption that SSL and TLS would be used to ***replace*** IPSec. The better interpretation is that SSL and TLS would be used to ***supplement*** IPSec. That interpretation accords with the specification's teaching that IPSec is essential, whereas MPH's interpretation finds no support in the specification (which never suggests replacing IPSec with SSL or TLS).

**4. If the "secure" terms in the Intermediate Computer Patents are not construed to require IPSec, they should be found indefinite.**

The "secure" terms are indefinite if not limited to IPSec because their scope lacks reasonable certainty. Claim terms are indefinite if their scope cannot be determined with "reasonable certainty" when read in light of the specification and prosecution history. *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014). Subjective claim terms are often found indefinite. *See, e.g.*, *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1363-64 (Fed. Cir. 2018) ("minimal redundancy" indefinite); *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1372 (Fed. Cir. 2014) ("unobtrusive manner" indefinite); *Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1350-52 (Fed. Cir. 2005) ("aesthetically pleasing" indefinite). ‼

Neither the specification nor file history discusses what it means to be "secure." MPH's position that "secure" means "protected by one or more security protocols" fails for two reasons. First, no intrinsic evidence supports that position. Rather, the specification says that "[t]he IP security protocols (***IPSec***) provides the capability to ***secure*** communications between arbitrary hosts . . . ." ('949 patent, 1:43-44.) Second, the term "security protocol" is itself indefinite if not

limited to IPSec, because there is no reasonable certainty as to how much or what type of security a "security protocol" requires. Thus, the "secure" terms are indefinite if not limited to IPSec.[5]

**5. The "secure" terms in the '581 and '302 patents also should be construed to require IPSec or otherwise as indefinite.**

The "secure" terms in the '581 and '302 patents present similar issues. The '581 patent's Summary of the Invention states: "In ***the invention***, the first terminal is movable from one network to another. Such a terminal can physically be a mobile terminal or a fixed terminal. The secure connection is an ***IPSec*** connection established by forming one or more Security Associations (SAs) using the ***IPSec*** protocols." ('581 patent, 6:59-64.) The '302 patent's Summary states that "in the solution of ***the invention***, an ***IPSec*** security association is used" and that "[t]he invention" provides advantages that include "***IPSec*** key management" and "***IPSec*** symmetric encryption and authentication." ('302 patent, 8:45-58; *see also id.*, 10:7-10 ("In the method of the invention, an ***IPSec*** tunnel mode or transport mode security association is used . . . .").) These statements limit the claims to IPSec for the reasons discussed above.

Like the specification of the Intermediate Computer Patents, the specifications of the '581 and '302 patents do not explain what "secure" means if it does not require IPSec. Therefore, the "secure" terms of the '581 and '302 patents should be found indefinite if not limited to IPSec.

**B. "Unique identity" (Intermediate Computer Patents)**

| MPH's Construction | Apple's Construction |
|---|---|
| Plain and ordinary meaning, no construction required.<br><br>Alternatively: "one or more parameters that can be used to find a destination address" | "One or more SPI values"<br><br>otherwise indefinite |

The term "unique identity" should be construed as "one or more SPI values" for three reasons. First, the applicants repeatedly represented that the invention uses SPI values. *See, e.g.*,

[5] MPH fails to address the indefiniteness of the "secure" terms in its opening brief. The Joint Claim Construction Statement expresses Apple's indefiniteness position with respect to the term "secure message." (Dkt. No. 92 at 8.) Due to a clerical error, the Statement does not express Apple's indefiniteness positions with respect to the other "secure" term, but Apple did disclose those positions in its Patent Local Rule 4-2 disclosures. (*See* Ex. Bat 1.)

*GPNE*, 830 F.3d at 1371. The specification states: "In ***the invention***, . . . the intermediate computer holds information required to perform address and IPSec ***SPI translations*** for the packets." ('949 patent, 10:11-14.) During prosecution, the applicants stated: "One unique feature of ***the present invention*** is that the intermediate computer modifies the addresses and ***SPI values*** of the same pre-existing secure connection i.e. without requiring the setting up of a new secure connection." (Ex. C at 8-9 ('949 history, June 29, 2009).) Twice later they argued: "In ***the current invention***, the intermediate computer . . . is able to use the outer IP addresses and the incoming ***SPI value (= unique identity).***" (Ex. D at 10 ('949 history, April 7, 2011); *id*., Ex. E at 10-11 ('949 history, November 7, 2011).)

Second, the applicants acted as their own lexicographers to define "unique identity" as SPI values. *See Jack Guttman, Inc. v. Kopykake Enters., Inc.*, 302 F.3d 1352, 1360-61 (Fed. Cir. 2002) ("Where, as here, the patentee has clearly defined a claim term, that definition usually is dispositive; it is the single best guide to the meaning of a disputed term." (internal quotation marks omitted)); *Honeywell Inc. v. Victor Co. of Japan*, 298 F.3d 1317, 1323 (Fed. Cir. 2002) ("It is well settled that a patentee may define a claim term either in the written description of the patent or, as in the present case, in the prosecution history."). Specifically, their statement that "***SPI value (= unique identity)***" constitutes a definition. (Ex. D at 10 ('949 history, April 7, 2011), Ex. E at 11 (November 7, 2011).)

Third, claim 10 recites: "[t]he method of claim 1 wherein the method further comprises changing both the address and ***the SPI-value*** by the intermediate computer." The term "***the*** SPI-value" lacks an antecedent basis if "unique identity" is not construed to require an SPI value. *See Comcast*, 38 F. Supp. 3d at 616.[6]

[6] Apple acknowledges that its proposed construction of "unique identity" differs from its proposed construction in its 2019 IPRs. MPH's briefing, however, confirms that a more precise construction is necessary. In defending its proposed construction, MPH disputes whether a "unique identity" can encompass parameters unrelated to IPsec. (D.I. 95 at 12.) As Apple has explained in connection with the "secure" terms, MPH is incorrect. Apple therefore provides an unambiguous construction of "unique identity" consistent with the intrinsic record: "one or more SPI values." MPH does not claim any prejudice from Apple's construction as clarified, and there is none. As MPH concedes, the PTAB did not construe "unique identity" during the IPR

If "unique identity" is not limited to SPI values, then it should be found indefinite because there is no reasonable certainty as to scope of the term. *See Nautilus*, 572 U.S. at 901. The specification does not explain what it means to be an "unique identity." Furthermore, the claims provide inconsistent answers to the question: *Identity of what?* In particular, '949 claim 1 recites a "unique identity of *the secure connection*," whereas '362 claim 1 recites a "unique identity of *the first computer*." MPH's proposed construction—"one or more parameters that can be used to find a destination address"—fails to answer that question and also conveys nothing about what it means for an identity to be "unique." The only way to provide a definite construction of "unique identity" is to limit it to SPI values.[7]

### C. "Exchanging keys with one another" / "key exchange protocol" (Intermediate Computer Patents)

| Claim Term | MPH's Construction | Apple's Construction |
|---|---|---|
| **"exchanging keys with one another"** | "establishing cryptographic keys not revealed to the intermediate computer" | "A computer sending a key to another computer in response to receiving a key from that computer" |
| **"key exchange protocol"** | "protocol for establishing cryptographic keys" | "Protocol for one computer to send a key to another computer in response to receiving a key from that computer" |

Because the parties seem to agree that the constructions of "key exchange protocol" and "exchanging keys with one another" are linked, Apple addresses these terms together. The parties disagree over whether exchanging keys requires actually exchanging keys between two computers (Apple's construction), as opposed to only "establishing" keys (MPH's construction).

In addition to the claim language itself, the specification confirms Apple's construction. Every instance in the specification of "exchanging keys with one another" shows an actual

---

proceedings. (Br. at 12.) That is in part because MPH stated during the IPRs: "The Board is correct that there is no reason to construe this term; its construction is not material to the grounds at issue." ('502 POR at 18.) When MPH made that statement, it expressly recognized that Apple's "apparent goal [was] to have 'unique identity' [be] . . . limited to the ***IPSec security protocol***." (*Id.* at 18-19.) Thus, MPH does not and cannot argue estoppel. *See Oxygenator Water Techs., Inc. v. Tennant Co.*, No. 20-cv-358, 2021 WL 3661587, at *4 (D. Minn. Aug. 18, 2021).

[7] MPH fails to address the term's indefiniteness in its opening brief even though the Joint Claim Construction Statement discloses Apple's indefiniteness position. (Dkt. No. 92 at 10.)

exchange of keys. For example, as depicted in Figure 4 of the '949 patent (annotated below), the second computer sends its key exchange data to the first computer after it receives key exchange data from the first computer. At step 5 (annotated in orange), the first computer sends the second computer a message with "[a] Key Exchange (KE) payload, that contains Diffie-Hellman key exchange data of the first computer." ('949 patent, 18:38-39.) At step 7 (annotated in purple), the second computer "***receives*** [the message] and ***responds*** with [its own message]" with "Key Exchange (KE) payload, that contains Diffie-Hellman key exchange data of the second computer." (*Id.*, 18:48-51.)

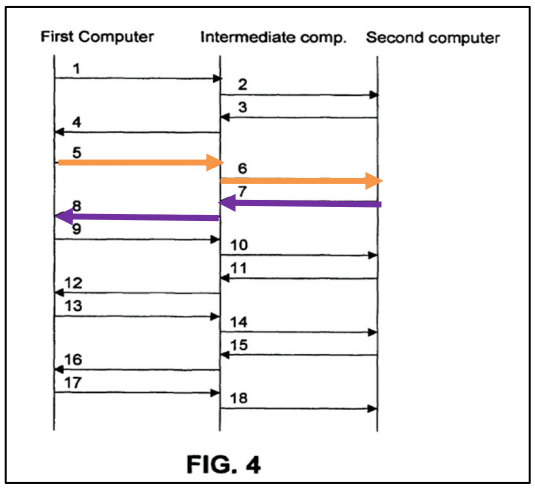

FIG. 4

The prosecution history further supports Apple's construction. The applicants argued that prior art "fail[ed] to teach or suggest the ***direct exchange of keys***" as there was "no direct exchange between the 25 client [(the first computer)] and the server [(the second computer)] to establish a tunnel between the client 405 to the server 440." (Ex. F at 11 ('949 history, November 16, 2010).) "Consistent with the public notice function of the prosecution history, the public is entitled to rely on these statements as defining the scope of the claims." *Data Engine Techs. LLC v. Google LLC*, 10 F.4th 1375, 1383; *MBO Labs., Inc. v. Becton, Dickinson & Co.*, 474 F.3d 1323, 1330 (Fed. Cir. 2007). Apple's construction comports with the "direct exchange" requirement, whereas MPH's does not.

General purpose dictionaries confirm Apple's position that an "exchange" comprises acts of giving and receiving. (*See* Ex. G, The American Heritage Dictionary of the English Language,

5th ed. ("exchange" means "to give and receive reciprocally" or "to give in return for something received."); Ex. H, Merriam-Webster.com Dictionary ("exchange" means "the act of giving or taking one thing in return for another").) MPH provides no basis for deviating from this commonly understood meaning of "exchange."

MPH asserts that "'exchanging keys with one another' merely means that the first and second computers establish cryptographic keys *without revealing them to the intermediate computer*." (Br. at 17 (emphasis in original).) This assertion is baseless. For one thing, MPH ignores that "exchanging" and "establishing" are not synonyms and that the phrase "with one another" reinforces that an exchange requires interaction. In addition, MPH provides no legal basis for injecting the phrase "without revealing them to the intermediate computer" into its construction of these terms. A different claim limitation recites that "the intermediate computer does not have the cryptographic key to decrypt the encrypted data payload." (*See* '362 claim 1.)

MPH erroneously relies on RFC 2412's statement that "***[t]he goal*** of key exchange processing is the secure establishment of common keying information state in the two parties." (Br. at 16 (citing RFC 2412).) The issue here is not the goal of a key exchange, but rather what the exchange ***is***. RFC 2412 supports Apple's construction on that issue. RFC 2412 explains that "roundtrips [are] needed for the keying material determination." (Br. at Ex. 26, RFC 2412 at 7.) Specifically, "the Initiator of the exchange begins by specifying as much information as he wishes in his first message. The Responder ***replies***, supplying as much information as he wishes. The two sides ***exchange*** messages, supplying more information each time, until their requirements are satisfied." (*Id.*) Thus, the computers participating in the exchange do not simply "establish[] cryptographic keys" as stated in MPH's construction.

MPH's reliance on *Applied Cryptography* is misplaced for the same reason. (Br. at 16 (citing Ex. 27).[8]) That a key exchange ***results*** in keys being "agreed upon" does not mean that the agreement ***is*** the exchange. Regardless, extrinsic evidence cannot change the meaning of "key exchange" established by the specification and file history. *See Phillips*, 415 F.3d at 1319.

[8] MPH did fail to disclose this reference in its August 3, 2023, Patent L.R. 4-2 Disclosures. (*See* Dkt. No. 92.) Apple's position is that MPH should not be permitted to rely on it.

The Court should not allow MPH to read the word "exchange" out of these terms that explicitly require an exchange. The Court should adopt Apple's constructions.

**D. "Negotiating" ('949 claim 1 and '397 claim 1)**

| MPH's Construction | Apple's Construction |
|---|---|
| "agreeing on cryptographic keys" | "Conferring to reach agreement on the parameters for a secure connection" |

The first question for the Court is whether "negotiating" means "agreeing" (as MPH proposes) or "conferring to reach agreement" (as Apple proposes). The second question is whether the negotiation is solely for cryptographic keys (as MPH proposes) or for the parameters of a secure connection more generally (as Apple proposes). Apple is right on both issues.

The specification explains that two computers confer with each other to set up the parameters for a secure connection—just as stated in Apple's construction. ('949 patent, FIG. 4 (annotated below).) The first computer begins by sending an offer to the second computer (step 1, shown in green). (*Id.*, 16:35-48.) The second computer can choose to accept or decline the offer. If it accepts, then it sends a reply (step 3, shown in blue) that "indicates which security configuration is acceptable for the second computer." (*Id.*, 17:67-18:1.) The first computer then responds with its parameters needed to form the secure connection, including not only the first computer's key but also other parameters (step 5, shown in orange). (*Id.*, 18:36-44.) The second computer does the same, responding with its key and other parameters (step 7, shown in purple). (*Id.*, 18:48-54.)

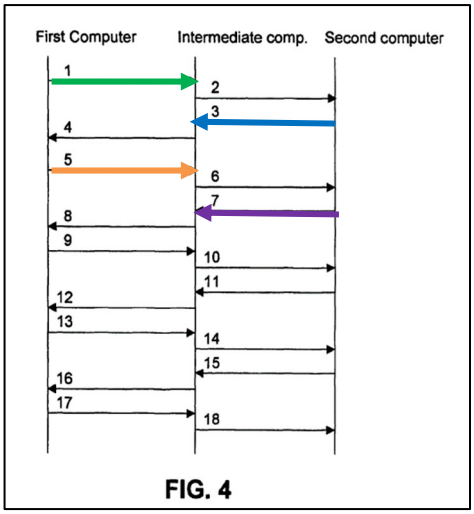

FIG. 4

Extrinsic evidence also supports Apple's construction. General purpose dictionaries define "negotiate" to mean conferring. (*See* Ex. I, The American Heritage Dictionary of the English Language, 5th ed. (negotiate: "***[t]o confer*** with another or others in order to come to terms or reach an agreement."); Ex. J, Merriam-Webster.com Dictionary (negotiate: "***to confer*** with another so as to arrive at the settlement of some matter").) Furthermore, a computer networking textbook from the timeframe of the alleged invention explained that "negotiating" referred to conferring on several parameters for a secure connection (not just keys). (Ex. K (Andrew S. Tanenbaum, *Computer Networks 4th ed*. (2003)), 32 ("In some cases when a connection is established, the sender, receiver, and subnet conduct a ***negotiation about parameters to be used***, such as maximum message size, quality of service required, and other issues. Typically, one side makes a proposal and the other side can accept it, reject it, or make a counterproposal."), 602 ("When the system is brought up, each pair of firewalls has to ***negotiate the parameters of its SA***, ***including the services, modes, algorithms, and keys***").)

MPH offers no support for its proposed construction. MPH points to the applicants' assertion during prosecution that "the nodes involved in the negotiation and exchange of keys according to the key exchange protocol IKE determines the boundaries of the secure connection." (Br. at 17 (citing '949 pat. file hist., 2010-06-22 Appeal Br., pp. 17–18.).) But nothing in this assertion suggests, as MPH contends, that negotiation can occur without interaction.

MPH also cites an extrinsic reference RFC 2412, but this reference undermines MPH's position.[9] Just as Figure 4 of the '949 patent shows a back-and-forth conferring process between two negotiating computers, RFC 2412 describes "roundtrips needed for the keying material determination." (Dkt. No. 95-27, RFC 2412.) Additionally, RFC 2412 discloses that the two negotiating computers confer on more parameters than just keys. (*Id.*, RFC 2412 ("The goal of key exchange processing is the secure establishment of common keying information state in the two parties. This state information is a key name, secret keying material, the identification of the

[9] The other extrinsic reference MPH cites, a cryptography textbook, does not mention "negotiation"; it only discusses a key exchange. (*See* Br. at Ex. 27, *Applied Cryptography*.) MPH did not disclose this reference in its August 3, 2023, Patent L.R. 4-2 Disclosures, which Apple objected to as untimely and prejudicial. (Dkt. No. 92.)

two parties, and three algorithms for use during authentication . . . "); *id*. (referring to document describing "how to ***negotiate acceptable parameter sets***").)

**E. "Negotiating and exchanging keys with one another, by the first and second computer, according to a key exchange protocol to establish the secure connection between the first computer and the second computer <u>via the intermediate computer</u>" ('949 claim 1)**

| MPH's Construction | Apple's Construction |
|---|---|
| "via the intermediate computer" modifies "the secure connection between the first computer and the second computer" | "Exchanging keys with one another via the intermediate computer" (i.e., the phrase "via the intermediate computer" modifies "exchanging keys with one another") |

The claim language presents an ambiguity: whether "via the intermediate computer" modifies the phrase "the secure connection between the first computer and the second computer" or the phrase "exchanging keys with one another." The intrinsic record confirms it is the latter.

All negotiations and key exchanges in the Intermediate Computer Patents occur via the intermediate computer.[10] The specification explains that "the overall key exchange [is] performed by the ***first, intermediate, and second computer***." ('949 patent, 14:22-24.) "The first computer initiates the key exchange protocol by sending a message to the intermediate computer." (*Id.* at 15:16-17.) "The intermediate computer determines which security gateway (second computer) to forward this [initiation message] to." (*Id*. at 15:21-23.) "The security gateway (the second computer) replies to the [] initiation message." (*Id*. at 15:26-27.) "The intermediate computer completes the IKE [(internet key exchange)] mapping based on the reply message." (*Id*. at 15:28-29.)

[10] (*See also* '949 patent, 10:39-43 ("For performing said key exchange, a standard IKE protocol is used between the server 2 [(the intermediate computer)]and the security gateway 3 [(the second computer)], and a modified IKE protocol is used between the client computer 1 [(the first computer)] and the server 2 [(the intermediate computer)].").)

Furthermore, all figures illustrating the key exchange process between the first and second computer show it occurring through the intermediate computer. (*See* '949 patent, 10:39-43 ("In the example of FIG. 1, . . . For performing said key exchange, a standard IKE protocol is used between the server 2 [(the intermediate computer)] and the security gateway 3 [(the second computer)], and a modified IKE protocol is used between the client computer 1 [(the first computer)] and the server 2 [(the intermediate computer)]."). For example, Figure 4 of the '949 patent shows a negotiation and exchange between the first and second computer through the intermediate computer at steps 5-8. ('949 patent, Fig. 4 (annotated below).) The first computer sends its "key exchange data" (shown in red) through the intermediate computer, and the second computer replies by sending its "key exchange data" (shown in blue) through the intermediate computer. (*Id.* at 18:36-51.)

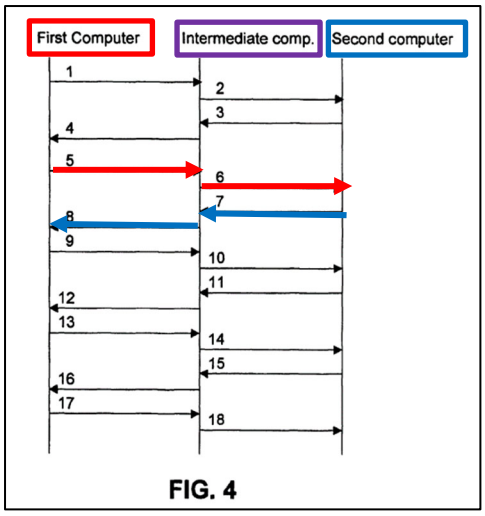

FIG. 4

The prosecution history of the '949 patent provides even more conclusive evidence that "via the intermediate computer" modifies the phrase "exchanging keys with one another." The examiner found "that [the prior art] teaches a direct key exchange between a first computer (client in [the prior art]) and a second computer (server in [the prior art]). (Ex. D at 13 ('949 history, April 7, 2011).) The applicants distinguished the prior art by arguing that the key exchange "takes place between the client and the gateway [(intermediate computer)] . . . and **not** between the client and the server ***via the gateway***, ***as required by the amended claim 1***." (*Id.* at 14.) Thus, the applicants explicitly stated that claim 1 ***requires*** that the key exchange occur via the intermediate computer. "Prosecution arguments . . . which draw distinctions between the

patented invention and the prior art . . . indicate in the inventor's own words what the invention is not." *MBO Labs., Inc.*, 474 F.3d at 1330; *see also Shire Dev., LLC v. Watson Pharms., Inc.*, 746 F.3d 1326, 1332 (Fed. Cir. 2014) (finding that prosecution history statements "inform[ed] the claim construction" and did not need to "rise to the level of unmistakable disavowal").

**F. "Intermediate computer" / "computer" (Intermediate Computer Patents)**

| Claim Term | MPH's Construction | Apple's Construction |
|---|---|---|
| **"intermediate computer"** | Plain and ordinary meaning, no construction required.<br>Alternatively: "an intermediate networking device (such as a server) comprising a stand-alone unit or interconnected units functioning together to facilitate secure communication between computers" | Original: "One intermediate computer (not a system of computers)"<br><br>Proposed modification: "At least one intermediate computer that individually satisfies each recited requirement on the intermediate computer"[11] |
| **"computer"** | Plain and ordinary meaning, no construction required. | "One intermediate computer (not a system of computers)"<br><br>Proposed modification: "At least one computer that individually satisfies each recited requirement on the computer" |

The claims of the Intermediate Computer Patents impose multiple requirements on an "intermediate computer" or "computer," including various activities that the computer must perform. For example, '949 claim 1 recites: "***the intermediate computer*** receiving the secure message and performing a translation"; "***the intermediate computer*** substituting the first destination address with the second destination address"; "substituting, at ***the intermediate computer***, the first unique identity with a second unique identity"; and "forwarding, at ***the intermediate computer***, the secure message." The question for the Court is whether these activities must be performed by the same single computer (as Apple contends) or instead can be performed by a network of different computers (as MPH contends).

[11] Apple proposes modifications to clarify its constructions for the reasons explained below.

The Federal Circuit considered the same issue in *Traxcell Techs., LLC v. Nokia Sols. & Networks Oy*, 15 F.4th 1136 (Fed. Cir. 2021). The claims there "recite[d] a 'computer' or 'first computer' capable of taking certain actions." *Id.* at 1143. "The question [was] whether these capabilities all belong to one computer or can be spread among multiple." *Id.* The Federal Circuit affirmed the district court's holding that one computer was required, explaining:

> As a matter of plain language, reciting "a computer" (or a "first computer") that performs a function, and then further reciting that "*the* computer" (or "*said* first computer") performs multiple additional functions, suggests that such "computer" must be tied to all those functions. And it would make little sense—indeed, it would defy the concept of antecedent basis—for the claims to recite "the computer" or "said first computer" being "further" programmed to do a second set of tasks if a different computer were to do those tasks instead.

*Id.* at 1143-44 (emphasis in original).

Similarly here, it would make little sense for the claims to recite that "***the*** intermediate computer" performs multiple activities if those activities could be performed by multiple computers. The applicants used a different word—"network"—to refer to multiple computers. For example, '949 claim 1 recites "an intermediate computer in a telecommunication network," which implies that the intermediate computer is one component in the broader network of computers. Consistently, the specification states that a "local area *network* (LAN)" "typically connects workstations, personal ***computers***, printers and other devices." ('949 patent, 1:19-21.)

MPH's reliance on cases holding that "a" or "an" means "one or more" is misplaced. (*See* Br. at 19-20.) The Federal Circuit recently explained why in *Salazar v. AT&T Mobility LLC*, 64 F.4th 1311 (Fed. Cir. 2023). The claims in *Salazar* recited "a microprocessor" in which "said microprocessor" performed various activities. *Id.* at 1313. The patentee argued that "a correct claim construction would encompass one microprocessor capable of performing one claimed function and another microprocessor capable of performing a different claimed function, even if no one microprocessor could perform all of the recited functions." *Id.* at 1315. The Federal Circuit disagreed. *Id.* at 1315-18. The court acknowledged that "a microprocessor" meant "one or more microprocessors," citing two of the cases cited by MPH. *Id.* at 1315-16 (citing *Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338 (Fed. Cir. 2008); *KCJ Corp. v. Kinetic Concepts, Inc.*, 223 F.3d 1351, 1356 (Fed. Cir. 2000)). Nonetheless, the court held that "it does

not suffice to have multiple microprocessors, each able to perform just one of the recited functions; the claim language requires at least one microprocessor capable of performing each of the recited functions." *Id.* at 1318. The court explained by analogy: "for a dog owner to have 'a dog that rolls over and fetches sticks,' it does not suffice that he have two dogs, each able to perform just one of the tasks." *Id.* (quoting *In re Varma*, 816 F.3d 1352, 1363 (Fed. Cir. 2016)).

To avoid any ambiguity, Apple also proposes a modified construction of these terms: "At least one [intermediate] computer that individually satisfies each recited requirement on the [intermediate] computer." Apple's modified construction is not intended to be a substantive change from its original proposed construction. Instead, Apple's proposed modified construction clarifies its position that, consistent with *Salazar*, the claims require that at least one computer individually satisfy each recited requirement for the "intermediate computer." *Salazar*, 64 F.4th at 1315-18; *Traxcell*, 15 F.4th at 1143-44.

MPH's proposed construction—covering "interconnected units functioning together to facilitate secure communication between computers"—should be rejected. This language appears nowhere in the specification and instead stems from dictionary definitions divorced from the issue at hand. That a computer can comprise interconnected units (*e.g.*, a microprocessor, a hard drive, etc.) does not support MPH's effort to extend "computer" to a network of different computers.

Therefore, the Court should adopt Apple's construction (as clarified above).

**G. "The intermediate computer configured to receive from a [mobile / second] computer a secure message sent to the first network address" ('494 claim 1 and '362 claim 1)**

| MPH's Construction | Apple's Construction |
|---|---|
| "The intermediate computer configured to receive a secure message sent from a [mobile / second] computer to the first network address" | "The intermediate computer configured to receive a secure message that a [mobile / second] computer sent to the first network address" |

The parties' dispute regarding this term is nuanced but important. The parties disagree about whether the intermediate computer receives a message that the mobile / second computer sent ***directly*** to it (Apple's construction), or whether the intermediate computer simply needs to receive a message that was sent ***passively*** from the mobile / second computer (MPH's

construction). MPH's construction would cover any message "***passively sent*** from a [mobile / second] computer" so long as it reaches an intermediate computer eventually, even though that message was not directly addressed to the intermediate computer from the mobile / second computer. (Br. at 23.) That proposed construction is inconsistent with the Federal Circuit's construction of this term, MPH's own arguments in that appeal, and the intrinsic record.

The Federal Circuit already decided that the claims require direct sending. On appeal from the PTAB's final written decision on the '494 patent IPR, the Federal Circuit explained: "The plain meaning of 'intermediate computer configured to receive from a mobile computer a secure message sent to the first network address' requires the mobile computer to send the message to the first network address. . . . ***The plain language establishes direct sending***." *Apple Inc. v. MPH Techs. Oy*, 28 F.4th 254, 261 (Fed. Cir. 2022).

The Federal Circuit found that "the written description confirms this plain meaning." *Id*. "It describes how the mobile computer forms the secure message with '***the destination address*** . . . ***of the intermediate computer***." *Id*. (citing '494 patent at 6:56-58, 11:32-33). "The mobile computer then sends the message to that address." *Id*. (citing '494 patent at 6:58-63). "***There is no passthrough destination address*** in the intermediate computer that the secure message is sent to before the first destination address." *Id*.

MPH contorts the Federal Circuit's opinion to argue that it supports MPH's passive sending construction because it "recognized the claims' use of passive language." (Br. at 24.) But the Federal Circuit explicitly found that "the claims use passive voice is of no import. The plain language established direct sending." *MPH*, 28 F.4th at 261.

MPH also incorrectly claims that its construction "mirrors" the Federal Circuit's explanation that "the written description describes the secure message as sent from the [mobile/second] computer ***directly*** to the first destination address." (Br. at 24 (citing *MPH*, 28 F.4th at 261).) But MPH's construction—purportedly "describing the 'secure message [as] sent from a [mobile/second] computer to the first network address'"—omits a critical word from the Federal Circuit's language: "directly."

Furthermore, MPH defended a construction requiring direct sending in its appellate briefing. In particular, MPH agreed with the PTAB's finding that the challenged limitation "***require[s]*** that the mobile computer send messages '***directly***' to the first network address [(the intermediate computer)]," asserting that the PTAB "applied [the claims'] plain meaning." *Apple Inc. v. MPH Techs. Oy*, No. 21-1532, Dkt. No. 23 at 19 (Aug. 18, 2021). MPH's statements are part of the intrinsic record here. *Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1362 (Fed. Cir. 2017) (patentee's statements during IPR proceedings are part of the prosecution history); *Springs Window Fashions LP v. Nova Indus., L.P.*, 323 F.3d 989, 995 (Fed. Cir. 2003) ("[t]he public notice function of a patent and its prosecution history requires that a patentee be held to what he declares during the prosecution of his patent.").

MPH provides no basis for this Court to deviate from the Federal Circuit's construction of this term. The Court should adopt that construction (as stated in Apple's proposal).

**H. "Establishing a secure connection having a first address of the mobile terminal as a first endpoint and a gateway address of the security gateway as a second endpoint … the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway" ('581 claim 1)**

| MPH's Construction | Apple's Construction |
|---|---|
| same as claim language and adds: [wherein the secure connection is between the mobile terminal and the security gateway protecting the other terminal] | Indefinite |

This term is indefinite because (1) the bounds of the "secure connection" are unclear given the lack of proper antecedent basis; and (2) it requires an impossibility.

The "secure connection" is defined in the first part of the term as "having a first address of the mobile terminal as the first end-point and a gateway address of the security gateway as the second end-point"—in other words, the secure connection starts at the mobile terminal and ends at the security gateway. The last limitation, however, refers to "the secure connection from the second address of the mobile terminal to the other terminal via the security gateway," which requires that the secure connection extend from the mobile terminal ***beyond*** the security gateway to "the other terminal." The secure connection of the last limitation is not the same secure connection as the antecedent basis "a secure connection."

"[A] claim could be indefinite if a term does not have proper antecedent basis where such basis is not otherwise present by implication or the meaning is not reasonably ascertainable." *Halliburton Energy Servs., Inc. v. M-I LLC*, 514 F.3d 1244, 1249 (Fed. Cir. 2008). A claim limitation lacks antecedent basis "where it would be unclear as to what element the limitation was making reference." *Baldwin*, 512 F.3d at 1343. For instance, "if two different levers are recited earlier in [a] claim, the recitation of 'said lever' in the same or subsequent claim would be unclear where it is uncertain which of the two levers was intended." *Id*.

Here, worse than in *Baldwin*, the secure connection is redefined and changed throughout the claim. The secure connection is first defined in limitation 1(a) as between the first address of the mobile terminal to the security gateway. It then changes in limitation 1(c) to "the secure connection to be defined between the second address [of the mobile terminal] to the gateway address." And in the last limitation, the secure connection extends from "the second address of the mobile terminal to the other terminal via the security gateway." Because of these multiple uses of "secure connection," it is unclear where the secure connection begins and ends.

This term is also indefinite because it requires an impossibility. *See Synchronoss Techs., Inc. v. Dropbox, Inc*., 987 F.3d 1358, 1366–67 (Fed. Cir. 2021) (holding claims indefinite where they were nonsensical and required an impossibility). The term requires that "the mobile terminal send[] a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway." But the term also says that the secure connection stops at the security gateway and does not reach the other terminal. It would therefore be impossible to send a secure message in the secure connection to the other terminal.

Contrary to MPH's contention, the disputed term cannot simply be understood by referring back to the secure connection "having a first address of the mobile terminal as a first end-point and a gateway address of the security gateway as a second end-point" (Br. at 5), especially in the context of the surrounding claim language. As the preamble states, the claimed method is "for ensuring secure forwarding of a message." MPH's reading of the claim language in an attempt to save this term from indefiniteness makes it impossible to ensure secure forwarding of a message. MPH relies on the specification to argue that the "connection between

the security gateway and the other terminal may be . . . unsecure 'plaintext'" (Br. at 5). But sending ***unsecure*** plaintext from the security gateway to the other terminal cannot "ensure secure forwarding of a message."

Moreover, MPH's reliance on only Figure 1 is misplaced. Figure 1 is just an example of a telecommunication network "***to be used*** in the invention." It does not describe the method of the invention itself. Rather, FIG. 5 is what "describes the ***method of the invention*** to enable to ***mobility*** for IPSec connections." MPH ignores that, as explicitly stated in claim 1(c), the secure connection changes to be defined between the first address and the gateway to between the second address and the gateway address of the security gateway, and then from "the second address of the mobile terminal to the other terminal via the security gateway," per the last limitation—changes that Figure 1 does not contemplate or address at all. Nothing in the claim language or the prosecution history suggests that any part of securely forwarding a message per the claims would entail sending unsecured plain text.

Because the "secure connection" lacks proper antecedent basis, making the bounds of the secure connection unclear, and the asserted claims are nonsensical and require impossibility, those skilled in the art cannot determine the scope of the invention with reasonable certainty. This claim term is therefore indefinite.

### I. "Wherein the computer is a mobile computer in that the address of the mobile computer changes" ('502 claim 1)

| MPH's Construction | Apple's Construction |
|---|---|
| "wherein the computer is a computer capable of moving between networks in that the address of the computer can change" | Indefinite |

The Federal Circuit "has held that 'reciting both an apparatus and a method of using that apparatus renders a claim indefinite under section 112, paragraph 2.'" *Rembrandt Data Techs., LP v. AOL, LLC*, 641 F.3d 1331, 1339 (Fed. Cir. 2011) (quoting *IPXL Holdings, L.L.C. v. Amazon.com, Inc.*, 430 F.3d 1377, 1384 (Fed. Cir. 2005)). In *Rembrandt*, the disputed claim recited "[a] data transmitting device for transmitting signals" and "transmitting the trellis encoded frames." *Id.* at 1339. The court found the claim indefinite because it recited the "transmitting"

step in an apparatus claim. *Id.* '502 claim 1 is indefinite for that reason. The claim is an apparatus claim directed to "[a] computer for sending messages." But the limitation at issue recites a step in using the computer—changing its address. This creates an ambiguity as to whether the claim is infringed upon making a computer capable of changing addresses or when a computer actually changes addresses. *See IPXL*, 430 F.3d at 1384.

MPH misreads this limitation as a functional limitation that describes the mobile computer's ***capability***. (Br. at 25.) But as MPH acknowledges, the term "mobile computer" alone already connotes "a computer that is ***capable*** of moving between networks." (Br. at 24.) The phrase "***the address of the mobile computer changes***" recites something more—an action that the mobile computer actually performs. That is impermissible in an apparatus claim.

MPH improperly attempts to redraft this limitation by adding the word "can" in front of "change" in its proposed construction. The patentee in *Rembrandt* tried to do the same thing. 641 F.3d at 1339. The Federal Circuit rejected that effort, explaining that "courts may not redraft claims, whether to make them operable or to sustain their validity." *Id.* (quoting *Chef Am., Inc. v. Lamb–Weston, Inc.*, 358 F.3d 1371, 1374 (Fed. Cir. 2004)). The same is true here. MPH cannot add "can" to this limitation. If the intent of the applicants was to connote capability, then they were required to include language like "can" or "capable of."

Therefore, the Court should find this limitation indefinite.

## V. CONCLUSION

Apple's proposed constructions correctly apply Supreme Court and Federal Circuit law to the claim language and intrinsic evidence at issue here. MPH's constructions deviate from the claim language and intrinsic evidence in an effort to ensnare ideas that the applicants for its patents did not invent. Therefore, the Court should adopt Apple's constructions.

Dated: November 2, 2023

MORRISON & FOERSTER LLP

By: */s/ Ryan J. Malloy*
Ryan J. Malloy

BITA RAHEBI
RYAN J. MALLOY
ROSE S. LEE
NIMA KIAEI
MORRISON & FOERSTER LLP
707 Wilshire Boulevard
Los Angeles, California 90017-3543
Telephone: (213) 892-5200
Facsimile: (213) 892-5454
brahebi@mofo.com
rmalloy@mofo.com
roselee@mofo.com
nkiaei@mofo.com

RICHARD S.J. HUNG
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105
Telephone: (415) 268-7000
Facsimile: (415) 268-7522
rhung@mofo.com

Attorneys for Defendant
APPLE INC.